



TITLE:

Polynomial Codeの構造について  
(情報理論・実験計画法における組  
合せ数学の諸問題Ⅱ: 研究会報告集  
)

AUTHOR(S):

浜田, 昇

---

CITATION:

浜田, 昇. Polynomial Codeの構造について (情報理論・実験計画法にお  
ける組合せ数学の諸問題Ⅱ: 研究会報告集). 数理解析研究所講究録  
1970, 95: 12-22

ISSUE DATE:

1970-08

URL:

<http://hdl.handle.net/2433/108171>

RIGHT:

## Polynomial code の構造について

愛媛大学 理 浜 田 昇

## § 1. 序

前回, 有限射影幾何  $PG(t, P^n)$  における点と  $d$ -flats からなる incidence matrix  $N_P$  や  $EG(t, P^n)$  における点と  $d$ -flats からなる incidence matrix  $N_E$  の  $GF(P^n)$  上での rank を求め, incidence matrix  $N_P$  を parity check matrix とする  $d$ -th order Projective Geometry code や incidence matrix  $N_E$  を parity check matrix とする  $d$ -th order Affine Geometry code の構造を明らかにした [3]。

今回は, 前回と同様な方法を用いて, これらの geometry codes を特別な場合として含む polynomial code の構造を明らかにする。

## § 2. Polynomial code の定義とその構造

$X_1, X_2, \dots, X_m$  を  $GF(q^A)$  上の値を取る  $m$  個の変数とし、  
次の 2 条件をみたす  $X_1, X_2, \dots, X_m$  の多項式：

$$f(X_1, X_2, \dots, X_m) = \sum_{\nu_1, \dots, \nu_m} c_{\nu_1, \nu_2, \dots, \nu_m} X_1^{\nu_1} X_2^{\nu_2} \dots X_m^{\nu_m} \quad (2.1)$$

の全体を  $P(m, A, \mu, b)$  で表わす。すなわち、

$$P(m, A, \mu, b) = \left\{ f(X_1, X_2, \dots, X_m) \left| \begin{array}{l} (2.1) \text{ のタイプで, (条件1),} \\ (条件2) \text{ をみたすもの} \end{array} \right. \right\}$$

(条件1) 係数  $c_{\nu_1, \nu_2, \dots, \nu_m}$  はすべて  $GF(q^A)$  の元である。

(条件2) 各項のべき： $\nu_1, \nu_2, \dots, \nu_m$  の和はすべて  $b$  の倍数で、かつ、 $\mu b$  より大きくなることはないこと。

$$\text{i.e., } \sum_{i=1}^m \nu_i = j b \quad (j = 0, 1, \dots, \mu-1 \text{ or } \mu) \quad (2.2)$$

ここに、 $\mu$  は非負の与えられた整数で、 $b$  は  $(q^A - 1)$  の約数である。以下、

$$Z = (q^A - 1) / b, \quad n = (q^{Am} - 1) / b \quad (2.3)$$

と置く。  $X_i^{q^A} = X_i$  ( $i = 1, 2, \dots, m$ ) であるから、以下、  
 $\nu_i$  ( $i = 1, 2, \dots, m$ ),  $\mu$  は

$$0 \leq \nu_i \leq q^A - 1, \quad 0 \leq \mu < mZ \quad (2.4)$$

をみたす整数とする。

$P(m, n, \mu, b)$  に属する多項式  $f(x_1, x_2, \dots, x_m)$  (以下,  $f(\bar{x})$  と略記する) に対して,  $GF(q^a)$  の元を要素とする  $n$  次元ベクトル空間  $W(n; q^a)$  のベクトル  $\underline{v} = (v_0, v_1, \dots, v_{n-1})$  を次のように対応させる。

$$\sigma : f(\bar{x}) \in P(m, n, \mu, b) \longrightarrow \underline{v} \in W(n; q^a) \quad (2.5)$$

ここに,  $\underline{v} = (v_0, v_1, \dots, v_{n-1})$  の  $j$  番目の要素  $v_j$  は

$$v_j = f(a_{1j}, a_{2j}, \dots, a_{mj}) \quad (j = 0, 1, \dots, n-1) \quad (2.6)$$

で与えられ,  $(a_{1j}, a_{2j}, \dots, a_{mj})$  は,  $\alpha$  を  $GF(q^{am})$  の原始元とする時,  $GF(q^{am})$  の元  $\alpha^j$  ( $j = 0, 1, \dots, n-1$ ) の座標表現である。すなわち,  $\alpha^j$  を  $\alpha^0, \alpha^1, \dots, \alpha^{m-1}$  で表わした時の係数,

$$\alpha^j = \sum_{i=1}^m a_{ij} \alpha^{i-1} \quad (j = 0, 1, \dots, n-1) \quad (2.7)$$

である。(もちろん,  $a_{1j}, a_{2j}, \dots, a_{mj}$  は  $GF(q^a)$  の元である。)

$\sigma$  による  $f(\bar{x})$  の像を  $\underline{v}(f)$  で表わし,

$$W_0 = \{ \underline{v}(f) \mid f(\bar{x}) \in P(m, n, \mu, b) \} \quad (2.8)$$

とみると,  $\sigma$  は  $P(m, n, \mu, b)$  から  $W_0$  の上への 1 対 1 対応。

である。

特に,  $W(n; q^0)$  でなく,  $W(n; q)$  のベクトルに対応する  $P(m, \Delta, \mu, b)$  の多項式  $f(\bar{x})$  の全体を  $Q(m, \Delta, \mu, b, q)$  で表わす。 すなわち,

$$Q(m, \Delta, \mu, b, q) = \left\{ f(\bar{x}) \in P(m, \Delta, \mu, b) \mid \begin{array}{l} f(a_j, \dots, a_{m_j}) \in GF(q) \\ \text{for } j=0, 1, \dots, n-1 \end{array} \right\}$$

とする。

$$V_0 = \{ \underline{v}(f) \mid f(\bar{x}) \in Q(m, \Delta, \mu, b, q) \} \quad (2.9)$$

とあくと,  $V_0$  は  $W(n; q)$  のベクトル部分空間を作る。

(定義)  $W(n; q)$  のベクトルのうちで,  $V_0$  に属するベクトル  $\underline{v}(f)$  だけを符号とする線形符号 (linear code) のことを  $(n, m, \Delta, \mu, q)$ -多項式符号 (polynomial code) という。

これについては, 嵩, Shu Lin, Peterson [1] による次の定理が成り立つ。

(定理 2.1) (a)  $(n, m, \Delta, \mu, q)$ -多項式符号は cyclic code である。

(b)  $\alpha$  を  $GF(q^{\Delta m})$  の原始元とすれば,  $(n, m, \Delta, \mu, q)$ -

多項式符号を生成する生成多項式  $g(x)$  の根は,  $\alpha^h$  のタイプのものに限る。ここに,  $h$  は  $0 \leq h < q^{\Delta m} - 1$  なる整数である。

(c)  $\alpha^h$  ( $0 \leq h < q^{\Delta m} - 1$ ) が  $(n, m, \Delta, \mu, q)$ -多項式符号の生成多項式  $g(x)$  の根であるための必要かつ十分条件は

$h$  が次の2条件をみたす整数であることである。

(条件1)  $h$  は  $b$  の倍数であること。

(条件2)  $h$  は  $\Delta$  個の整数値  $W_{q^{\Delta}}(h), W_{q^{\Delta}}(h q), \dots, W_{q^{\Delta}}(h q^{\Delta-1})$

のうちの最小値が  $b$  の倍数で, かつ,  $0$  より大きく,  $(m\Delta - \mu)b$  より小さくなるような整数であること。i.e.,  $h$  は

$$\min_{0 \leq l < \Delta} W_{q^{\Delta}}(h q^l) = j b \quad (\text{但し, } 0 < j < m\Delta - \mu) \quad (2.10)$$

をみたす整数  $j$  が存在するような整数であること。

ここに,  $W_{q^{\Delta}}(H)$  は, (1)  $0 \leq H < q^{\Delta m} - 1$  なる整数  $H$  に対しては,  $H$  の  $q^{\Delta}$  進数表示を

$$H = \delta_1 + \delta_2 q^{\Delta} + \dots + \delta_m q^{(m-1)\Delta} \quad (0 \leq \delta_i < q^{\Delta})$$

とするとき,

$$W_{q^{\Delta}}(H) = \delta_1 + \delta_2 + \dots + \delta_m \quad (2.11)$$

を意味し, (2)  $H \geq q^{\Delta m} - 1$  なる整数  $H$  に対しては,  $H$  を  $(q^{\Delta m} - 1)$  で割った時の余りを  $H_0$  とするとき,  $W_{q^{\Delta}}(H) = W_{q^{\Delta}}(H_0)$

を意味する。

(系 2.1) (a)  $(n, m, \lambda, \mu, q)$ -多項式符号の dual code は cyclic code である。

(b)  $\alpha^h$  ( $0 \leq h < q^{\lambda m} - 1$ ) が  $(n, m, \lambda, \mu, q)$ -多項式符号の生成多項式  $g_0(x)$  の根であるための必要かつ十分条件は,  $h$  が次の条件をみたす整数であることである。

(条件 1)  $h$  は  $b$  の倍数であること。

(条件 2)  $h$  は

$$\max_{0 \leq l < \lambda} W_{g^{\lambda}}(h q^l) = j b \quad (0 \leq j \leq \mu) \quad (2.12)$$

をみたす整数  $j$  が存在するような整数であること。

この note の目的は, これらの定理と前回の方法を用いて,  $(n, m, \lambda, \mu, q)$ -多項式符号の information symbol の数を求めることである。

まず, 次の補題が成り立つ。(詳しくは論文[2]参照)

(補題 2.1)  $h$  を  $0 \leq h < q^{\lambda m} - 1$  なる整数とし,  $h$  の  $q$  進表示を

$$h = \sum_{i=0}^{m-1} \sum_{j=0}^{\lambda-1} c_{ij} q^{i\lambda+j} \quad (0 \leq c_{ij} < q) \quad (2.13)$$

とする。このとき、 $h$  が  $b$  の倍数、すなわち、 $(q^A - 1)/\varepsilon$  の倍数であるならば、次の条件をみたす整数の組  $(p_0, p_1, \dots, p_A)$  がただ一組存在する。 i.e.,  $j = 0, 1, \dots, A-1$  に対して、

$$\text{(条件)} \quad \begin{cases} p_A = p_0, \quad 0 \leq p_j < m\varepsilon & (2.14) \\ \varepsilon \sum_{i=0}^{m-1} c_{ij} = p_{j+1}q - p_j & (2.14') \end{cases}$$

をみたす整数の組  $(p_0, p_1, \dots, p_A)$  がただ一組存在する。

$c_{ij}$  は  $0 \leq c_{ij} \leq q-1$  なる整数であるから、(2.14') は  $(p_{j+1}q - p_j)/\varepsilon$  ( $j=0, 1, \dots, A-1$ ) が

$$0 \leq (p_{j+1}q - p_j)/\varepsilon \leq m(q-1) \quad (2.15)$$

をみたす整数であることを示す。

(補題 2.2) 逆に、 $(p_0, p_1, \dots, p_A)$  を次の条件：

$$\text{(条件)} \quad \begin{cases} p_A = p_0, \quad 0 \leq p_j < m\varepsilon \\ (p_{j+1}q - p_j)/\varepsilon \text{ は整数, かつ} \\ 0 \leq (p_{j+1}q - p_j)/\varepsilon \leq m(q-1) \end{cases} \quad (2.16)$$

( $j=0, 1, \dots, A-1$ ) をみたす整数の組とすると、

(i)  $0 \leq c_{ij} < q$  ( $i=0, 1, \dots, m-1, j=0, 1, \dots, A-1$ ) で、かつ、

$$\sum_{i=0}^{m-1} c_{ij} = (p_{j+1}q - p_j)/\varepsilon \quad (2.17)$$



( $j = 0, 1, \dots, \lambda-1$ ) をみたす整数の組  $\{c_{ij}\}$  が少なくとも一組存在する。

(ii) (2.17) をみたす任意の整数の組  $\{c_{ij}\}$  に対して,

$$h = \sum_{i=0}^{m-1} \sum_{j=0}^{\lambda-1} c_{ij} g^{i\lambda+j} \quad (2.18)$$

とあくと,  $h$  は  $b$  の倍数で, かつ,  $0 \leq h < g^{\lambda m} - 1$  なる整数である。

(iii) このとき,  $l = 0, 1, \dots, \lambda-1$  に対して,

$$W_{g^\lambda}(h g^l) = p_{\lambda-l} b \quad (2.19)$$

が成り立つ。

従って, 定理 2.1 の条件は

$$0 < \min(p_1, p_2, \dots, p_\lambda) < m\lambda - \mu \quad (2.20)$$

を意味する。従って, 次の定理が成り立つ。

(定理 2.2)  $(p_0, p_1, \dots, p_\lambda)$  を (2.16) と (2.20) の条件をみたす任意の整数の組とする。このとき,

$\{c_{ij} : i=0, 1, \dots, m-1, j=0, 1, \dots, \lambda-1\}$  を (2.17) をみたす任意の整数の組とし, (2.18) で  $h$  を定義すると,  $\alpha^h$  は  $(n, m, \lambda, \mu, g)$ -多項式符号の生成多項式  $g(x)$  の根である。逆に,

$g(x)$  の根は上のタイプのものに限る。

$$0 \leq \max \{ p_1, p_2, \dots, p_d \} \leq \mu \quad (2.21)$$

とあくと, (系 2.1) より, 次の系が成り立つ。

(系 2.2)  $(p_0, p_1, \dots, p_d)$  を (2.16) と (2.21) の条件をみたす任意の整数の組とする。このとき,  $\{c_{ij}\}$  を (2.17) をみたす任意の整数の組とし, (2.18) で  $h$  を定義すると,  $\alpha^h$  は  $(n, m, d, \mu, q)$ -多項式符号の dual code の生成多項式  $g_0(x)$  の根である。逆に,  $g_0(x)$  の根は上のタイプのものに限る。

一般に, cyclic な linear code の information symbol の数はその dual code を生成する生成多項式の根の数に等しい。

従って,  $(n, m, d, \mu, q)$ -多項式符号の information symbol の数は  $(n, m, d, \mu, q)$ -多項式符号の dual code を生成する生成多項式  $g_0(x)$  の根の数に等しい。以下,  $g_0(x)$  の根の数を求める。

条件 (2.16) と (2.21) は合せて次のようにかける。

$$(\text{条件}) \quad \begin{cases} p_d = p_0, \quad 0 \leq p_j \leq \mu \\ (p_{j+1}q - p_j)/\varepsilon \text{ は 整数, かつ} \\ 0 \leq (p_{j+1}q - p_j)/\varepsilon \leq m(q-1) \end{cases} \quad (2.22)$$

前回と同様な方法 ([2], [3] 参照) を用いて, 系 2.2 より  
次の結果をうる。

(定理 2.3)  $(n, m, \rho, \mu, q)$ -多項式符号の information  
symbol の数は次式によって与えられる。

$$\sum_{p_0} \cdots \sum_{p_{\rho-1}} \prod_{j=0}^{\rho-1} \sum_{i=0}^{L(p_{j+1}, p_j)} (-1)^i \binom{m}{i} \binom{m-1+(p_{j+1}q-p_j)/q-iq}{m-1} \quad (2.23)$$

ここに,  $p_\rho = p_0$  で,  $\sum_{p_0} \cdots \sum_{p_{\rho-1}}$  は (2.22) の条件をみた  
すすすべての整数の系組  $(p_0, p_1, \dots, p_{\rho-1})$  に対する和を表わし,  
 $L(p_{j+1}, p_j)$  は  $(p_{j+1}q - p_j)/q$  を越えない最大の整数を表わ  
す。

### 参 考 文 献

[1] Kasami, T., Shu Lin and Peterson, W. W. (1968).

Polynomial codes.

IEEE Transactions on information theory IT-14 807-814.

[2] Hamada, N. (1968). The rank of the incidence  
matrix of points and  $d$ -flats in finite geometries.

J. Sci. Hiroshima Univ. Ser. A-I 32 381-396.

- [3] 浜田 昇 (1970). 有限幾何における点と  $d$ -flats からの incidence matrix の rank と majority decodable code について.

数理解析研究所 講究録 82.